AD-A017 852

MESSAGE RECEIPT PROBABILITIES

Theodore M. Hardebeck, et al

Air Force Weapons Laboratory
Kirtland Air Force Base, New Mexico

November 1975

338145

AFWL-TR-75-172

AFWL-TR-75-172

ADA017852

MESSAGE RECEIPT PROBABILITIES

Theodore M. Hardeback, Lt, USAF
John M. Kamm, Jr.
Air Force Weapons Laboratory (SAS)
Kirtland Air Force Base, NM 87117

November 1975

Final Report

Approved for public release; distribution unlimited.

AIR FORCE WEAPONS LABORATORY
Air Force Systems Command
Kirtland Air Force Base, NM 87117

27

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER AFWL-TR-75-172	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) MESSAGE RECEIPT PROBABILITIES		5. TYPE OF REPORT & PERIOD COVERED Final Report
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Theodore M. Hardebeck, Lt, USAF John M. Kamm, JR.		8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS Air Force Weapons Laboratory (SAS) Kirtland Air Force Base, NM 87117		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS 62601F 88090450
11. CONTROLLING OFFICE NAME AND ADDRESS Air Force Weapons Laboratory Air Force Systems Command Kirtland Air Force Base, NM 87117		12. REPORT DATE November 1975
		13. NUMBER OF PAGES 27
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) Unclassified
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Character error rate
Signal-to-noise ratio
Phonetic letters spelled out
Message probabilities

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

A method for evaluating digital communication systems performance is given. This method involves calculating the probability that a formatted message transmitted by the system is correctly received. Communication systems which employ radio wave propagation are susceptible to degradation of the propagated signal. Degradation of the signal occurs even in normal conditions because of various disturbances to the medium through which the signal passes. Nuclear detonation, far more so, produce severe disturbances. There are mathematical models incorporated in computer codes which assist in rapid calculation of various quantities

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

BLK 20

used to describe degradation. These quantities include: signal absorption and signal to noise ratio. For the commander, these quantities do not answer the main question which is will the system perform its mission. This report is an attempt to bridge the gap between the output of the system codes and the data required for command decisions. To do this, the probability of receiving a correct message is calculated. This message probability is an easily understood measure of system performance upon which command decisions can be based.

This report was prepared for the Air Force Weapons Laboratory. Captain Jesus S. Tirado (SAS) was the Laboratory Project Officer-in-Charge.

When US Government drawings, specifications, or other data are used for any purpose other than a definitely related Government procurement operation, the Government thereby incurs no responsibility nor any obligation whatsoever, and the fact that the Government may have formulated, furnished or in any way supplied the said drawings, specifications, or other data, is not to be regarded by implication or otherwise, as in any manner licensing the holder or any other person or corporation, or conveying any rights or permission to manufacture, use, or sell any patented invention that may in any way be related thereto.

This report has been reviewed by the Information Office (OI) and is releasable to the National Technical Information Service (NTIS). At NTIS, it will be available to the general public, including foreign nations.

This technical report has been reviewed and is approved for publication.

JESUS S. TIRADO
Captain, USAF
Project Officer

FOR THE COMMANDER

WAYNE L. TYLER
Lt. Colonel, USAF
Chief, System S/V Support Branch

PAUL J. DAILY
Colonel, USAF
Chief, Analysis Division

ACCESSION for
NTIS White Section ☑
DDC Buff Section ☐
UNANNOUNCED ☐
JUSTIFICATION
BY
DISTRIBUTION/AVAILABILITY CODES
Dist. AVAIL. and/or SPECIAL
A

DO NOT RETURN THIS COPY. RETAIN OR DESTROY.

PREFACE

The technique for calculating the probability of accepting a false phonetic letter was developed by Ms. R. Dillard, Naval Electronic Laboratory Center, San Diego, California.

CONTENTS

Section		Page
I	INTRODUCTION	5
II	INITIAL DEVELOPMENT	8
III	PHONETIC LETTERS SPELLED OUT	11
IV	REPETITION	14
V	MESSAGE PROBABILITIES	15
VI	EXAMPLE	17
	APPENDIX A	23
	APPENDIX B	24
	ABBREVIATIONS AND SYMBOLS	25

SECTION I

INTRODUCTION

Communications systems which employ radio wave propagation are susceptible to degradation of the propagated signal. Degradation of the signal occurs even in normal conditions because of various disturbances to the medium through which the signal passes. Nuclear detonations, far more so, produce severe disturbances, such as abnormal signal attenuation, dispersion, refractive effects, phase shift, time delay, and polarization rotation. In this document, only the degradation effects occurring in the medium between the transmitting and receiving antennas will be considered. Further, the analysis will address only systems which transmit a formatted message in digital form. To emphasize, no hardware response will be considered.

There are mathematical models incorporated in computer codes which assist in rapid calculation of the various quantities used to describe degradation. The output of such a code will be used in this work to calculate probabilities which measure the performance of the system to transmit messages accurately. Here, it is assumed that the transmitter and receiver are working perfectly, and the goal is to describe how precisely the information obtained by the receiver matches that information inserted into the transmitter.

A receiver, having processed the received signal, will output a message in a coded format which, hopefully, is the same as the one transmitted. This format may consist of groups of letters; here, each letter is called a character, and each group of characters is a character string. Generally, the character string, at its origin, spells out a coded alphanumeric word, such as BRAVO. The performance measurement will be to determine the probability that the operator on the receiver end will either receive this BRAVO character string or, at least, be able to interpret BRAVO, and nothing else. For example, if what he receives is RRAVO, he may be permitted to interpret this as BRAVO. The extent to which he is permitted to interpret is specifically defined to him and is called acceptance criteria. The criterion may be, as is implicit in the foregoing example, that he is allowed to interpret one wrong character in a string, e.g., the first character R as a B, since no other alphanumeric word could be interpreted reasonably.

Formatted messages are made up of a specific number of character strings. Further, each character string contains a specific number of characters. Hence, knowing both format and acceptance criteria, a formula can be derived which will give the probability that the correct message has been interpreted given that a perfect one is transmitted.

One other condition is possible, however. The character string can be garbled to the extent that it is interpreted, even under adequate acceptance criteria, as a different character string. For example, ALFA could be sent and ZULU interpreted. Again, a probability for a false character string and, hence, a false message accepted as correct can be derived, knowing format and criteria.

If these two probabilities are summed, the result is the probability that the operator will accept the message as correct after applying the acceptance criteria, even though the message may be false.

As mentioned before, it is assumed that any incorrect characters are a result of signal degradation and not a malfunction related to any part of the equipment. Hence, the performance measurement must incorporate such effects, and this is done through the relationship of the rate of character errors to each of the basic probabilities. Character error rate (CER) is defined as the ratio of the number of character errors to the total number of characters received, e.g., 10 character errors in every 10,000 characters sent, or a CER of 10^{-3}.

In turn, the CER is related to the signal to noise ratio (S/N) which, of course, is a measure of signal degradation through the medium. Without pursuing in detail, suffice it to say that a computer program is used to provide a S/N for a nuclear disturbed medium. The inputs would be those necessary to describe the energies from the detonations along a specific propagation path. The CER is found by entering the S/N into a system performance curve which correlates the S/N to CER; thus, the goal is attained. (For an example of a system performance curve, see reference 1.)

[1] Stein, S. and Jones, J.J., Modern Communication Principles, McGraw Hill, p.351, 1968.

It should be pointed out that the performance curve contains the character bit structure of the system, and any changes to that bit structure may significantly affect system performance.

The method of arriving at the goal will be straightforward. First, section II demonstrates how to compute the probability that a correct character string is interpreted (accepted), and also shows how to compute the probability that a false character string is accepted (assumed to be correct). The techniques for obtaining these two probabilities are the building blocks for all the remaining computations. The techniques are applied in section III to the specific case where the format is phonetic letters spelled out (PLSO) -- much the same as the earlier examples, e.g., ROMEO, ALPHA, BRAVO, etc. Section IV looks at the case where the format is strings of repeated characters, e.g., AAAA, BBBB, CCCC, etc. Finally, the efforts of sections II, III, and IV are combined in section V, which shows the calculation of specific message receipt probabilities.

To help clarify these procedures, an example of their application is given in section VI. Additionally, this section includes illustrations of different techniques of combining (piecing together) character strings from different transmissions of the same message. This is done to demonstrate message acceptance practices.

A complete list of PLSO is given in appendix A, and a listing of the 32 unshifted symbols which can be used in a standard teletype system is given in appendix B.

SECTION II
INITIAL DEVELOPMENT

In this section, the probability that a correct character string is accepted and the probability that a false character string is accepted are derived.

Suppose a message is transmitted that consists of character strings taken from an available set $A = \{\psi_j : j = 1, 2, \ldots, s\}$. Possiblities for A include: A = { ALFA , BRAVO, ..., ZULU}, A = {AAAA, BBBB, ..., ZZZZ}, or A = {ZERO, ONE, ..., NINE}. The number of characters in a character string is called the length of the character string. For example, the length of the character string ALFA is four. Let n_ℓ denote the number of character strings in A of length ℓ. Let z denote the character error rate; i.e., the probability that a single character is in error. In this report, the character errors are assumed to be independent; i.e., the possibility of a character being in error has no relationship to previous or subsequent character errors. An apparent character error is a character which the receiving operator perceives as being in error. For example; if only PLSO are transmitted and the character string KIMO is received, then M is an apparent character error. However, if LIMA was actually transmitted, the character M is not, in fact, in error; this is the reason for the adjective "apparent". If the acceptance criterion is that, at most, r apparent errors are permitted in a character string to accept it, then

$$
\begin{aligned}
&\Pr\begin{pmatrix}\text{accept correct character}\\ \text{string from set A}\end{pmatrix}\\
&= \sum_{\ell} \Pr\begin{pmatrix}\text{character string of}\\ \text{length } \ell \text{ transmittal}\end{pmatrix} \Pr_{r}\left(\begin{matrix}\text{accept correct}\\ \text{character string}\\ \text{from set A}\end{matrix}\,\middle|\,\begin{matrix}\text{character string}\\ \text{of length } \ell\\ \text{transmitted}\end{matrix}\right)\\
&= \sum_{\ell}\left[\Pr\begin{pmatrix}\text{character string of}\\ \text{length } \ell \text{ transmitted}\end{pmatrix} \sum_{j=0}^{r}\binom{\ell}{j}(1-z)^{\ell-j} z^{j}\right] \qquad (1)
\end{aligned}
$$

where

$$\binom{\ell}{j} = \frac{\ell!}{(\ell-j)!\ j!} \quad .$$

Note that $\Pr\begin{pmatrix}\text{character string of}\\ \text{length } \ell \text{ transmitted}\end{pmatrix} = \sum\limits_{\substack{i\\ \text{s.t.}\\ \text{length of } \psi_i = \ell}} \Pr(\psi_i \text{ transmitted}).$

Consider any particular character string; $\psi_j \in A$. Let ℓ_j denote the length of ψ_j. The distance between two character strings of the same length is the number of character positions in which they differ. For example, the distance between KILO and LIMA is three (KILO and LIMA differ in the first character position, $K \neq L$, the third character position $L \neq M$, and the fourth character position $O \neq A$). Let $n_{\psi_j}(d)$ denote the number of character strings in set A of length ℓ_j having a distance d from character string ψ_j. Let $n(\ell;d)$ denote the number of ordered pairs of character strings in A of length ℓ and distance d. Then, $n(\ell;d) = \sum\limits_{\substack{j\\ \text{s.t.}\\ \ell_j = \ell}} n_{\psi_j}(d).$

The probability of accepting a false character string is

$$\Pr\begin{pmatrix}\text{receiving any character string from set A of same length}\\ \text{but distinct from the character string transmitted}\end{pmatrix}$$

$$= \sum_j \Pr\left(\begin{matrix}\text{receiving character string}\\ \text{from set A of length } \ell_j \text{ but}\\ \text{distinct from } \psi_j\end{matrix} \,\middle|\, \psi_j \text{ transmitted}\right) \Pr(\psi_j \text{ transmitted})$$

$$= \sum_j \sum_h n_{\psi_j}(\ell_j - h) \Pr\left(\begin{matrix}\text{receiving a particular}\\ \text{character string from}\\ \text{set A of length } \ell_j \text{ and}\\ \text{distance } \ell_j - h \text{ from } \psi_j\end{matrix} \,\middle|\, \psi_j \text{ transmitted}\right) \Pr(\psi_j \text{ transmitted}) \tag{2}$$

If $\ell_j = \ell_i$, then we assume that

$$\Pr\left(\begin{matrix}\text{receiving a particular character string from}\\ \text{set A of length } \ell_j \text{ and distance } \ell_j - h \text{ from } \psi_j\end{matrix} \,\middle|\, \psi_j \text{ transmitted}\right)$$

$$= \Pr\left(\begin{matrix}\text{receiving a particular character string from}\\ \text{set A of length } \ell_i \text{ and distance } \ell_i - h \text{ from } \psi_i\end{matrix} \,\middle|\, \psi_i \text{ transmitted}\right).$$

(This assumption is made to reduce the complexity of the calculations. AFWL is in the process of calculating the probabilities from the bit error rate instead of the character error rate as in this study. The above assumption will not be made in our future work; however, no significant change in the results is expected.)

If we combine terms for ψ_j's of the same length, letting

$$\Pr(\text{A conversion} \mid \ell,h) = \Pr\left(\begin{array}{l}\text{receiving a particular}\\ \text{character string from}\\ \text{set A of length } \ell \text{ and}\\ \text{distance } \ell\text{-h from } \psi\end{array} \middle| \begin{array}{l}\psi \text{ of length}\\ \ell \text{ transmitted}\end{array}\right) \qquad (3)$$

(ψ denotes any character string from set A of length ℓ);

we have,

$$\Pr\left(\begin{array}{l}\text{receiving any character}\\ \text{string from set A of same}\\ \text{length but distinct from}\\ \text{that transmitted}\end{array}\right) = \sum_{\ell}\sum_{h} B(\ell,h)\Pr(\text{A conversion} \mid \ell,h) \qquad (4)$$

where

$$B(\ell,h) = \sum_{\substack{\psi_j \varepsilon A \\ \text{s.t.} \\ \ell_j = \ell}} n_{\psi_j}(\ell_j - h)\Pr(\psi_j \text{ transmitted})$$

A numerical example of the above calculation is given in section VI.

SECTION III

PHONETIC LETTERS SPELLED OUT

This section considers the special case where the message consists of phonetic letters spelled out (PLSO); i.e., A = {ALFA, BRAVO, ..., ZULU} = $\{\psi_j: j = 1, 2, \ldots, 26\}$. It is assumed in this section that each PLSO character string in the set A is equally likely to be transmitted. Also, it is assumed that the character transmission set (set of characters which can be transmitted by the system) is the 32 character teletype set as listed appendix B. In this case the relation between ℓ and n_ℓ is as follows:

ℓ	5	6	7	8	9
n_ℓ	9	7	5	4	1

The length, ℓ, includes one space since the possibility that the length of the phonetic letter is incorrectly interpreted because of a letter in the blank space is approximately accounted for by including the probability of incorrect reception of the space character in calculations. Also, the acceptance criterion assumed is that at most one apparent error is permitted in a character string to accept it. Hence, from (1) it follows that

$$\Pr\begin{pmatrix}\text{accept correct PLSO}\\ \text{character string}\end{pmatrix} = \frac{1}{26}\sum_{\ell=5}^{9} n_\ell\left[(1-z)^\ell + \ell(1-z)^{\ell-1} z\right] .$$

Recall that $n_{\psi_j}(d)$ is the number of character strings in A of length ℓ_j having distance d from ψ_j. For PLSO character strings, $n_{\psi_j}(d) \neq 0$ only for $d = \ell_j - 1$, $\ell_j - 2$, and $\ell_j - 3$. Hence, it follows from Eq (4) that

$$\Pr\begin{pmatrix}\text{accept false PLSO}\\ \text{character string}\end{pmatrix}$$

$$= \sum_{\ell=5}^{9} \sum_{h=1}^{3} B(\ell,h) \Pr\left(\begin{matrix}\text{receiving a particular}\\ \text{PLSO character string}\\ \text{of length } \ell \text{ and dis-}\\ \text{tance } \ell\text{-h from } \psi\end{matrix} \;\middle|\; \begin{matrix}\psi \text{ of length}\\ \ell \text{ transmitted}\end{matrix}\right)$$

where

$$B(\ell,h) = \sum_{\substack{\psi_j \in A \\ \text{s.t.} \\ \ell_j = \ell}} n_{\psi_j} (\ell_j - h) \frac{1}{26}$$

$$= \frac{1}{26} n(\ell;\ell-h)$$

The values of $n(\ell;\ell-h)$ for PLSO character strings are contained in the following table:

h	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
ℓ	9	9	9	8	8	8	7	7	7	6	6	6	5	5	5
$n(\ell;\ell-h)$	0	0	0	8	4	0	10	8	2	32	8	2	52	20	0

Examining Pr (PLSO conversion | ℓ, 2), see Eq (3) for notation, we have

$$\Pr\begin{pmatrix}\text{receiving particular PLSO character} \\ \text{string of length } \ell \text{ and distance } \ell-2\end{pmatrix}$$

$$= \Pr\begin{pmatrix}\text{receive a particular PLSO} \\ \text{character string of length} \\ \ell \text{ and distance } \ell-2 \text{ \underline{and} shared} \\ \text{character and space both} \\ \text{correct}\end{pmatrix} + \Pr\begin{pmatrix}\text{receive a particular PLSO} \\ \text{character string of length} \\ \ell \text{ and distance } \ell-2 \text{ \underline{and}} \\ \text{both not correct}\end{pmatrix}$$

Hence

Pr (PLSO conversion | ℓ,2)

$$= (1-z)^2 \sum_{i=0}^{1} \binom{\ell-2}{i} \left(\frac{z}{31}\right)^{\ell-2-i} \left[1 - \left(\frac{z}{31}\right)\right]^i + 2z\,(1-z) \left(\frac{z}{31}\right)^{\ell-2}$$

Here it has been assumed that if a character is in error, it is equally likely to be any of the other 31 characters. In a similar manner

Pr (PLSO conversion | ℓ, 1)

$$= (1-z) \sum_{i=0}^{1} \binom{\ell-1}{i} \left(\frac{z}{31}\right)^{\ell-1-i} \left[1 - \left(\frac{z}{31}\right)\right]^i + z \left(\frac{z}{31}\right)^{\ell-1}$$

and

Pr (PLSO conversion | ℓ, 3)

$$= (1-z)^3 \sum_{i=0}^{1} \binom{3}{i} \left(\frac{z}{31}\right)^{3-i} \left[1 - \left(\frac{z}{31}\right)\right]^i + 3z\,(1-z)^2 \left(\frac{z}{31}\right)^3 .$$

((HOTEL, ROMEO) is the only pair of PLSO that are identical in 3 character positions; O, E, and space.)

In this section, the assumption is made that all PLSO character strings are equally likely to be transmitted. In some applications this is not the case; however, the general procedure developed in Section II may be used to obtain useful results. The example in Section VI illustrates this.

SECTION IV

REPETITION

In this section it is assumed that the message consists of repetitive character strings; e.g., A = (AA...A, BB...B, ..., ZZ...Z) where each character string consists of M characters. As in Section III, the transmission set is assumed to be the 32 character teletype set. The acceptance criterion is that a character string is accepted if at least M-r of the M characters are identical. Hence,

$$\Pr\begin{pmatrix}\text{accept correct character}\\ \text{string from set A}\end{pmatrix} = \sum_{i=0}^{r} \binom{M}{i} (1-z)^{M-i} z^{i}$$

and

$$\Pr\begin{pmatrix}\text{accept false character}\\ \text{string from set A}\end{pmatrix} = \sum_{i=0}^{r} \left(\frac{25z}{31}\right)\left(\frac{z}{31}\right)^{M-1-i}\left(1-\frac{z}{31}\right)^{i}\binom{M}{i}$$

where

$\frac{25z}{31}$ is the probability of receiving a particular incorrect character which is one of the other 25 alphabetic characters.

SECTION V

MESSAGE PROBABILITIES

In this section the various character string probabilities are combined to calculate message probabilities. Suppose a character string taken from a set A is to be transmitted k times. Let x_i denote the probability that the correct character string is accepted in the i^{th} transmission. Let y_i denote the probability that a false character string is accepted in the i^{th} transmission. If the receiving operator is permitted to examine each record copy of the character string and if he selects the first acceptable copy to act upon (this method of character string combining (piecing) will be referred to later as unlimited), then

$$\Pr\begin{pmatrix}\text{accept the character}\\ \text{string in k transmissions}\end{pmatrix} = 1-\Pr\begin{pmatrix}\text{reject the character}\\ \text{string in all of the}\\ \text{k transmissions}\end{pmatrix} = 1-\prod_{i=1}^{k}(1-x_i-y_i)$$

Also,

$$\Pr\begin{pmatrix}\text{accept correct character}\\ \text{string in k transmissions}\end{pmatrix}$$

$$= \Pr\begin{pmatrix}\text{accept correct character}\\ \text{string in 1st transmission}\end{pmatrix}$$

$$+ \Pr\begin{pmatrix}\text{reject character string}\\ \text{in 1st transmission} & \text{and} & \text{accept correct character}\\ & & \text{string in 2nd transmission}\end{pmatrix}$$

$$+\ldots+\Pr\begin{pmatrix}\text{reject character}\\ \text{string and in 1st} & \text{and} & \text{accept correct character}\\ \text{(k-1) transmission} & & \text{string in } k^{th} \text{ transmission}\end{pmatrix}$$

$$= x_1 + x_2(1-x_1-y_1) + \ldots + x_k \prod_{i=1}^{k-1}(1-x_i-y_i)$$

It has been assumed in the above calculations that x_i/y_i and x_j/y_j, $i \neq j$ are independent. That is, the character string probabilities in a particular transmission are unaffected by the character string probabilities in previous transmissions.

Furthermore, assume that x_i/y_i are constant; i.e., $x_i = x$ and $y_i = y$ for all i, then

$$\Pr\begin{pmatrix}\text{accept correct character}\\ \text{string in k transmissions}\end{pmatrix} = x \sum_{j=0}^{k-1} (1-x-y)^j$$

$$= x\left[\frac{1-(1-x-y)^k}{1-(1-x-y)}\right]$$

$$= \frac{x}{x+y}\left[1-(1-x-y)^k\right]$$

If the message contains t character strings, each of which is taken from the same set A, then

$$\Pr\begin{pmatrix}\text{message is accepted}\\ \text{in k transmissions}\end{pmatrix} = \left[1-(1-x-y)^k\right]^t$$

and

$$\Pr\begin{pmatrix}\text{correct message is}\\ \text{accepted in k}\\ \text{transmissions}\end{pmatrix} = \left[\frac{x}{x+y}\left(1-(1-x-y)^k\right)\right]^t$$

Hence,

$$\Pr\begin{pmatrix}\text{false message is}\\ \text{accepted in k}\\ \text{transmission}\end{pmatrix} = \Pr\begin{pmatrix}\text{message is}\\ \text{accepted in k}\\ \text{transmissions}\end{pmatrix} - \Pr\begin{pmatrix}\text{correct message is}\\ \text{accepted in k}\\ \text{transmissions}\end{pmatrix}$$

$$= \left[1-(1-x-y)^k\right]^t - \left[\frac{x}{x+y}\left(1-(1-x-y)\right)^k\right]^t$$

$$= \left[1-\left(\frac{x}{x+y}\right)^t\right]\left[1-(1-x-y)^k\right]^t$$

Section VI contains a detailed example of the above calculations for a sample message.

SECTION VI

EXAMPLE

This section contains an example which will illustrate the procedures developed in the preceding sections. Suppose the following message consisting of five character strings is to be transmitted:

a. The first four character strings will be taken from the set {ALFA, BRAVO, ..., ZULU}; i.e., PLSO. Each character string in this set is equally likely to be transmitted.

b. The fifth character string will be taken from the set {ZERO, ONE, TWO}; each character string in this set is equally likely to be transmitted. The following table was computed using the methods developed in section III.

CER	$u=\Pr\begin{pmatrix}\text{Accept correct PLSO}\\ \text{character string}\end{pmatrix}$	$v=\Pr\begin{pmatrix}\text{Accept false PLSO}\\ \text{character string}\end{pmatrix}$
.001	1.0	2.636E-09
.01	.9983	2.589E-07
.05	.9633	5.964E-06
.075	.9237	1.273E-05
.1	.8748	2.144E-05
.15	.7601	4.314E-05
.2	.6368	6.815E-05

Using the techniques developed in section III, the associated probabilities for the fifth character string will be computed. It is assumed that at most one apparent character error is permitted in the fifth character string to accept it. Let A = {ZERO, ONE, TWO} = $\{\zeta_j,\ j = 1, 2, 3\}$. Let ℓ_j denote the length of ζ_j. As in PLSO character strings, the length includes one space. Hence

$$x = \Pr\begin{pmatrix}\text{accept correct 5th}\\ \text{character string}\end{pmatrix} = \frac{1}{3}\left[\left((1-z)^5 + 5(1-z)^4\ z\right) + 2\left((1-z)^4 + 4(1-z)^3\ z\right)\right].$$

The probability of accepting an incorrect fifth character string is

$$y = \Pr\begin{pmatrix}\text{receiving any character string from set A of}\\ \text{same length, but distinct from that transmitted}\end{pmatrix}$$

$$= \sum_{j=1}^{3} \Pr\left(\begin{array}{l}\text{receiving any character} \\ \text{string from set A of} \\ \text{length } \ell_j \text{ but distinct} \\ \text{from } \zeta_j\end{array} \middle| \ \zeta_j \text{ transmitted}\right) \Pr\left(\zeta_j \text{ transmitted}\right)$$

Note if $\ell_i = \ell_j$, then

$$\Pr\left(\begin{array}{l}\text{receiving a particular} \\ \text{character string from set} \\ \text{A of length } \ell_j \text{ and distance} \\ \ell_j\text{-1 from } \zeta_j\end{array} \middle| \ \zeta_j \text{ transmitted}\right)$$

$$= \Pr\left(\begin{array}{l}\text{receiving a particular} \\ \text{character string from set} \\ \text{A of length } \ell_i \text{ and distance} \\ \ell_i\text{-1 from } \zeta_i\end{array} \middle| \ \zeta_i \text{ transmitted}\right)$$

If we combine terms for ζ_j's of the same length, we have

$$y = \sum_{\ell=4}^{5} B(\ell,1) \Pr\left(\begin{array}{l}\text{receiving a particular} \\ \text{character string from} \\ \text{set A of length } \ell \text{ and} \\ \text{distance } \ell\text{-1 from } \zeta\end{array} \middle| \ \begin{array}{l}\zeta \text{ of length } \ell \\ \text{transmitted}\end{array}\right)$$

where

$$B(\ell 1) = \sum_{\substack{\zeta_j \\ \text{s.t.} \\ \ell_j = \ell}} \{A \quad n_{\zeta_j} \ (\ell_j\text{-1}) \ \Pr\ (\zeta_j \text{ transmitted})$$

and ζ denotes any character string of set A of length ℓ.

Since it was assumed that each character in set A is equally likely to be transmitted, it follows that Pr (ζ_i transmitted) = $\frac{1}{3}$ for all i. Also, the following table can be readily computed:

i	n_{ζ_i} (ℓ_i-1)
1	0
2	1
3	1

It follows from section III, that

$$Pr\left(\begin{array}{l}\text{receiving a particular}\\ \text{character string from}\\ \text{set A of length } \ell \text{ and}\\ \text{distance } \ell\text{-1 from } \zeta\end{array}\middle|\begin{array}{l}\zeta \text{ of length } \ell\\ \text{transmitted}\end{array}\right)$$

$$= (1-z)\sum_{i=0}^{1}\binom{\ell-1}{i}\left(\frac{z}{31}\right)^{\ell-1-i}\left(\frac{1-z}{31}\right)^{i} + z\left(\frac{z}{31}\right)^{\ell-1}$$

The following table was calculated using the above methods.

CER	x	y
0.001	1.0	2.08E-09
.01	.9993	2.06E-07
.05	.9831	4.93E-06
.075	.9636	1.08E-05
.1	.938	1.87E-05
.15	.8721	3.97E-05
.2	.7919	6.34E-05

Using the above probabilities, calculations will be made for the probability that the receiving operator accepts the message, the probability that the receiving operator accepts the correct message, and the probability that the receiving operator accepts a false message. Suppose the message is transmitted k times, and suppose the character strings are pieced together as in section V,(first paragraph), then

$$Pr\left(\begin{array}{l}\text{accept PLSO character}\\ \text{string in k transmissions}\end{array}\right) = 1-(1-u-v)^k ,$$

$$Pr\left(\begin{array}{l}\text{accept correct PLSO character}\\ \text{string in k transmissions}\end{array}\right) = \frac{u}{u+v}\left[1-(1-u-v)^k\right]$$

and

$$Pr\left(\begin{array}{l}\text{accept correct fifth character}\\ \text{string in k transmissions}\end{array}\right) = \frac{x}{x+y}\left[1-(1-x-y)^k\right]$$

Hence,

$$Pr\left(\begin{array}{l}\text{accept message in k}\\ \text{transmissions}\end{array}\right) = \left[1-(1-u-v)^k\right]^4\left[1-(1-x-y)^k\right]$$

and

$$Pr\left(\begin{array}{l}\text{accept correct message}\\ \text{in k transmissions}\end{array}\right) = \left[\left(\frac{u}{u+v}\right)\left(1-(1-u-v)^k\right)\right]^4\left[\left(\frac{x}{x+y}\right)\left(1-(1-x-y)^k\right)\right]$$

as before,

$$\Pr\begin{pmatrix}\text{accept false message}\\ \text{in K transmissions}\end{pmatrix} = \Pr\begin{pmatrix}\text{accept message in}\\ \text{k transmissions}\end{pmatrix} - \Pr\begin{pmatrix}\text{accept correct}\\ \text{message in k}\\ \text{transmissions}\end{pmatrix}$$

Substituting values for u, v, x, and y yields the following table

CER	k	Pr (accept message in k transmissions)	Pr (accept correct message in k transmissions)	Pr (accept false message in k transmissions)
0.001	2	0.100E+01	0.100E+01	0.126E-07
.001	4	.100E+01	.100E+01	.126E-07
.001	6	.100E+01	.100E+01	.126E-07
.01	2	.100E+01	.100E+01	.124E-05
.01	4	.100E+01	.100E+01	.124E-05
.01	6	.100E+01	.100E+01	.124E-05
.05	2	.994E+00	.994E+00	.296E-04
.05	4	.100E+01	.100E+01	.298E-04
.05	6	.100E+01	.100E+01	.298E-04
.075	2	.976E+00	.976E+00	.647E-04
.075	4	.100E+01	.100E+01	.663E-04
.075	6	.100E+01	.100E+01	.663E-04
.1	2	.935E+00	.935E+00	.110E-03
.1	4	.999E+00	.999E+00	.118E-03
.1	6	.100E+01	100E+01	.118E-03

Further, consider a case where the character string piecing is not unlimited (see sect V, first paragraph). Suppose the first three character strings are authenticators; i.e., the receiver is assumed to know what the first three character strings should be. The message acceptance criteria are as follows:

a. The authenticators must be correct in one record copy.

b. The remaining portion of the message may be pieced unlimitedly (as in section V).

Let

E = Event "all three authenticators are correct".

Hence

$$\Pr(E) = u^3$$

If the message is transmitted k times, then

$$Pr\begin{pmatrix}\text{E occurs at least once}\\ \text{in k transmissions}\end{pmatrix} = 1-(1-u^3)^k$$

Hence

$$Pr\begin{pmatrix}\text{accept message in}\\ \text{k transmissions}\end{pmatrix} = Pr\begin{pmatrix}\text{E occurs at least}\\ \text{once in k trans-}\\ \text{missions}\end{pmatrix} Pr\begin{pmatrix}\text{remainder of mes-}\\ \text{sage can be un-}\\ \text{limitedly pieced}\end{pmatrix}$$

$$= \left(1-(1-u^3)^k\right)\left(1-(1-u-v)^k\right)\left(1-(1-x-y)^k\right)$$

Likewise,

$$Pr\begin{pmatrix}\text{accept correct}\\ \text{message in k}\\ \text{transmissions}\end{pmatrix} = \left[1-(1-u^3)^k\right]\left[\left(\frac{u}{u+v}\right)\left(1-(1-u-v)^k\right)\right]\left[\left(\frac{x}{x+y}\right)\left(1-(1-x-y)^k\right)\right]$$

As before,

$$Pr\begin{pmatrix}\text{accept false message}\\ \text{in k transmissions}\end{pmatrix} = Pr\begin{pmatrix}\text{accept message in}\\ \text{k transmissions}\end{pmatrix} - Pr\begin{pmatrix}\text{accept correct}\\ \text{message in k}\\ \text{transmissions}\end{pmatrix}$$

Substituting values for u, v, x, and y yields the following table:

CER	k	Pr (accept message in k transmissions)	Pr (accept correct message in k transmissions)	Pr (accept false message in k transmissions)
0.001	2	1.0	1.0	0.472E-08
.001	4	1.0	1.0	.472E-08
.001	6	1.0	1.0	.472E-08
.01	2	1.0	1.0	.465E-06
.01	4	1.0	1.0	.465E-06
.01	6	1.0	1.0	.465E-06
.05	2	.987	.987	.111E-04
.05	4	1.0	1.0	.112E-04
.05	6	1.0	1.0	.112E-04
.075	2	.948	.948	.237E-04
.075	4	.998	.998	.249E-04
.075	6	1.0	1.0	.250E-04
.1	2	.873	.873	.388E-04
.1	4	.988	.988	.439E-04
.1	6	.999	.999	.444E-04

APPENDIX A

PHONETIC LETTERS SPELLED OUT

ALFA	NOVEMBER
BRAVO	OSCAR
CHARLIE	PAPA
DELTA	QUEBEC
ECHO	ROMEO
FOXTROT	SIERRA
GOLF	TANGO
HOTEL	UNIFORM
INDIA	VICTOR
JULIET	WHISKEY
KILO	XRAY
LIMA	YANKEE
MIKE	ZULU

APPENDIX B

UNSHIFTED TELETYPE CHARACTERS WITH ASSOCIATED BIT STRUCTURE

11000	A	11101	Q	
10011	B	01010	R	
01110	C	10100	S	
10010	D	00001	T	
10000	E	11100	U	
10110	F	01111	V	
01011	G	11001	W	
00101	H	10111	X	
01100	I	10101	Y	
11010	J	10001	Z	
11110	K	00010	<	
01001	L	01000	≡	
00111	M	11011	↑	(Shift)
00110	N	00100	-	(Space)
00011	O	00000	″	
01101	P	11111	↓	

ABBREVIATIONS & SYMBOLS

ψ_j = particular character string

A = $\{\psi_j : j = 1, \ldots, s\}$ = set of character strings

z = character error rate

ℓ_j = length of character string ψ_j

n_ℓ = number of character strings of length ℓ in A

The distance between two character strings of the same length in A is the number of character positions in which they differ.

$n_{\psi_j}(d)$ = number of character strings in A of length ℓ_j having d from ψ_j

$n(\ell;d)$ = number of ordered pairs of character strings in A of length ℓ and distance d